Available online at www.sciencedirect.com
ScienceDirect
Journal of Pure and Applied Algebra 210 (2007) 63–80
JOURNAL OF PURE AND APPLIED ALGEBRA
www.elsevier.com/locate/jpaa

On certain birational invariants of the Fermat curves

E. Kunz*, R. Waldi

Fakultät f. Mathematik, Universität Regensburg, 93040 Regensburg, Germany

Received 29 September 2005; received in revised form 1 August 2006
Available online 19 October 2006
Communicated by A.V. Geramita

Abstract

For an integer $m \geq 3$ let $K_m = \mathbb{Q}(x, y)$ $(x^m + y^m = 1)$ be the m-th Fermat field over $\mathbb{Q}$. We study, in the case of Fermat fields, the groups of integral differentials introduced by Kähler [E. Kähler, Geometria aritmetica, Annali di Mat. 45 (1958)] and Bost [R. Berndt, Arithmetisch ganze Differentiale, Abh. Math. Sem. Univ. Hamburg 47 (1978) 249–270] for arithmetic function fields and compute them for small m. An essential step of our considerations is the explicit description of the discrete valuation rings with quotient field K_m which are essentially of finite type and smooth over $\mathbb{Z}$.

MSC: Primary: 14F10; secondary: 11R58

1. Introduction

Let $K_m := \mathbf{Q}(x, y)$, $x^m + y^m = 1$ $(m \geq 3)$ be the field of rational functions of the Fermat curve over $\mathbf{Q}$, and let V be the set of all discrete valuation rings $(R, \mathfrak{m}_R)$ with $Q(R) = K_m$ which are essentially of finite type over $\mathbf{Z}$. Moreover let $V_s := \{R \in V \mid R \text{ is smooth over } \mathbf{Z}\}$. For $R \in V$ we denote the image of the canonical map $\Omega^1_{R/\mathbf{Z}} \to \Omega^1_{K_m/\mathbf{Q}}$ by $[R, \mathrm{d}R]^1$, and by $\mathfrak{d}_1(R/\mathbf{Z})$ the first Kähler different of $R/\mathbf{Z}$. For $R \in V_s$, since $\Omega^1_{R/\mathbf{Z}}$ is a free R-module, we can identify $[R, \mathrm{d}R]^1$ with $\Omega^1_{R/\mathbf{Z}}$, and we have $\mathfrak{d}_1(R/\mathbf{Z}) = R$. We are interested in the abelian groups

$$D^1(K_m) := \bigcap_{R \in V} [R, \mathrm{d}R]^1$$

$$D^1\left(\frac{K_m}{\mathfrak{d}}\right) := \bigcap_{R \in V} \frac{1}{\mathfrak{d}_1(R/\mathbf{Z})}[R, \mathrm{d}R]^1$$

and

$$D^1_s(K_m) := \bigcap_{R \in V_s} \Omega^1_{R/\mathbf{Z}}.$$

* Corresponding author.
E-mail addresses: ernst.kunz@mathematik.uni-regensburg.de (E. Kunz), rolf.waldi@mathematik.uni-regensburg.de (R. Waldi).

0022-4049/$ - see front matter © 2006 Elsevier B.V. All rights reserved.
doi:10.1016/j.jpaa.2006.08.016

In much greater generality the first two were introduced by Kähler [4], the last one by Bost [3]. Kähler showed that

$$D^1(K_m) = \left(\bigoplus_{i+k \le m-3} \mathbf{Z} x^i y^k \right) \omega \tag{1.1}$$

where $\omega := \frac{\mathrm{d}x}{y^{m-1}} = -\frac{\mathrm{d}y}{x^{m-1}}$, and in [5] we proved that

$$D^1\left(\frac{K_m}{\mathfrak{d}}\right) \subset \frac{1}{m} \left(\bigoplus_{i+k \le m-3} \mathbf{Z} x^i y^k \right) \omega \tag{1.2}$$

where equality holds if and only if m is squarefree. All three groups are free of rank $g := \binom{m-1}{2}$, the genus of K_m, and by definition

$$D^1(K_m) \subset D^1\left(\frac{K_m}{\mathfrak{d}}\right) \subset D_s^1(K_m). \tag{1.3}$$

Thus $D_s^1(K_m)/D^1(\frac{K_m}{\mathfrak{d}})$ and $D_s^1(K_m)/D^1(K_m)$ are finite abelian groups.

We want to derive some properties of these birational invariants of the Fermat curves and compute them for small m. To this end we first describe the elements of V_s and their modules of differentials explicitly, which will be done in Section 3. This section is based on a description of the discrete valuation rings of the rational function field $\mathbf{Q}(x)$ which are essentially of finite type and smooth over $\mathbf{Z}$, and of their modules of differentials (Section 2).

Section 4 contains what we can say about $D_s^1(K_m)$ and $D^1(\frac{K_m}{\mathfrak{d}})$ in general, and in Section 5 we compute $D_s^1(K_m)/D^1(K_m)$ and $D_s^1(K_m)/D^1(\frac{K_m}{\mathfrak{d}})$ for $m \le 6$.

In [6] we have studied the situation for elliptic curves defined over algebraic number fields.

2. Smooth discrete valuation rings of rational function fields of one variable and their modules of differentials

Let $(P, \mathfrak{m}_P)$ be a discrete valuation ring with quotient field k and perfect residue field $\mathfrak{k}(P)$. Further let π be a prime element of P. Assume that K/k is an algebraic function field of one variable which is separable, and let R be a discrete valuation ring with $Q(R) = K$ which dominates P and is essentially of finite type and smooth over P. Since R is flat over P smoothness simply means that $\mathfrak{m}_R = \pi R$. Equivalently $\Omega^1_{R/P}$ is a free R-module of rank 1:

$$\Omega^1_{R/P} = R\eta \subset \Omega^1_{K/k}$$

with some $\eta \in \Omega^1_{K/k}$. If v_R denotes the normed discrete valuation of K associated with R, then in particular the value $v_R(\omega)$ of each differential $\omega \in \Omega^1_{K/k}$ is defined, where $v_R(\eta) = 0$. Since $\Omega^1_{\mathfrak{k}(R)/\mathfrak{k}(P)} = \Omega^1_{R/P}/\pi\Omega^1_{R/P} \cong \mathfrak{k}(R)$ the residue field $\mathfrak{k}(R)$ has transcendence degree 1 over $\mathfrak{k}(P)$.

Let x be a separating transcendental element of K/k, that is $K/k(x)$ is a finite separable extension, or equivalently $\Omega^1_{K/k} = K\mathrm{d}x$. Let $R' := R \cap k(x)$ be the valuation ring of the restriction of v_R to $k(x)$. Then $\mathfrak{m}_{R'} = \pi R'$ and $\mathfrak{k}(R)/\mathfrak{k}(R')$ is algebraic. Further $x \in R'$ or $x^{-1} \in R'$. In the following we assume that $x \in R'$.

Set $\mathfrak{p} := \mathfrak{m}_R \cap P[x]$ and $P_0 := P[x]_{\mathfrak{p}}$. If $\mathfrak{p} = \pi P[x]$, then $R' = P_0$. Otherwise $\mathfrak{p} = \mathfrak{m}$ is a maximal ideal of $P[x]$ which contains π, and we have $P[x]/\mathfrak{m} = \mathfrak{k}(P)[\xi]$ with the residue ξ of x. If $f \in P[x]$ is a representative of the minimal polynomial of ξ over $\mathfrak{k}(P)$, then $\mathfrak{m} = (\pi, f)$, and $P_0 = P[x]_{\mathfrak{m}}$ is a two-dimensional regular local ring with $\mathfrak{k}(P_0) = \mathfrak{k}(P)[\xi]$. In particular $\mathfrak{k}(P_0)$ is a perfect field, and $\mathfrak{k}(R')/\mathfrak{k}(P_0)$ has transcendence degree 1.

The *quadratic sequence* over $P[x]$ along R' is defined as follows. Set $R_0 := P_0$. If $P_0 = R'$, then the sequence consists only of R_0. Otherwise R_0 is a two-dimensional regular local ring, and R_1 is defined as the local ring on the blowing up of the maximal ideal of R_0 which is dominated by R'. If R_i for some $i \ge 1$ is already constructed and $R_i \ne R'$, then R_{i+1} arises from R_i as R_1 did from R_0. By Abhyankar [1], Proposition 3, we have in our situation (but also more generally): the quadratic sequence

$$R_0 \subset R_1 \subset \cdots \subset R_i \subset \cdots$$

ends after finitely many steps with $R_s = R'$. We call the invariant s, which depends only on R' and $P[x]$, the *length* of the quadratic sequence which connects $P[x]$ with R'. We have $s = 0$ in the case $R' = P[x]_{(\pi)}$.

In the following proposition we determine the module of differentials $\Omega^1_{R'/P}$ and prove Abhyankar's result in our special situation.

Proposition 2.1. *R' is essentially of finite type over P, and we have*

$$\Omega^1_{R'/P} = R'\frac{\mathrm{d}x}{\pi^s}$$

where s is the length of the quadratic sequence connecting $P[x]$ with R'.

Proof. The assertions are clear if $R' = P[x]_{(\pi)}$. Otherwise $\mathfrak{m} = (\pi, f)$ as indicated above. Set $\alpha_1 := v_R(f)$ and $u_1 := \frac{f}{\pi^{\alpha_1}}$. Then $P_0[u_1] \subset R'$, and in $\Omega^1_{R/P}$ we have

$$\mathrm{d}u_1 = \frac{\mathrm{d}f}{\pi^{\alpha_1}}.$$

Since $f'(x)$ is a unit of R this implies $v_R(\mathrm{d}u_1) + \alpha_1 = v_R(\mathrm{d}x)$. But $v_R(\mathrm{d}u_1) \geq 0$, so we can choose f among the representatives of the minimal polynomial of ξ over $\mathfrak{k}(P)$ in such a way that its value α_1 is maximal.

$P_0[u_1]$ is obtained by blowing up the ideal (π^{α_1}, f) of P_0 which is generated by a regular sequence. Therefore

$$P_0[u_1] = P_0[U]/(\pi^{\alpha_1}U - f)$$

and since $f = \pi^{\alpha_1}u_1$ we have that

$$P_0[u_1]/\pi P_0[u_1] = \mathfrak{k}(P_0)[U]$$

is a polynomial ring over $\mathfrak{k}(P_0)$. When $\mathfrak{m}_R \cap P_0[u_1] = \pi P_0[u_1]$, then

$$R' = P_0[u_1]_{(\pi)}, \quad \mathfrak{k}(R') = \mathfrak{k}(P_0)(U), \quad \Omega^1_{R'/P} = R'\mathrm{d}u_1 = R'\frac{\mathrm{d}x}{\pi^{\alpha_1}}$$

and we are done since α_1 is the length of the quadratic sequence connecting $P[x]$ with R'.

Otherwise $\mathfrak{m}_R \cap P_0[u_1] =: \mathfrak{m}_1$ is a maximal ideal of $P_0[u_1]$, hence $\mathfrak{m}_1 = (\pi, g_1(u_1))$ with a representative $g_1 \in P_0[U]$ of the minimal polynomial of the residue ξ_1 of u_1 over $\mathfrak{k}(P_0)$. If we had $\xi_1 \in \mathfrak{k}(P_0)$ this minimal polynomial would be linear, that is $\bar{g}_1(U) = U - \bar{\rho}(\bar{\rho} \in \mathfrak{k}(P_0) = \mathfrak{k}(P)[\xi])$, where $\bar{g}_1$ is the reduction of g_1 modulo π. With a representative $\rho \in P[x]$ of $\bar{\rho}$ we had $v_R(u_1 - \rho) > 0$, hence $v_R(f - \pi^{\alpha_1}\rho) > \alpha_1$ contradicting the maximality property of f. Therefore if we set $P_1 := P_0[u_1]_{m_1}$, then $\mathfrak{k}(P_1)/\mathfrak{k}(P_0)$ is a separable extension with $[\mathfrak{k}(P_1) : \mathfrak{k}(P_0)] > 1$, and P_1 is again a two-dimensional regular local ring where P_1/P is smooth and $\Omega^1_{P_1/P} = P_1\mathrm{d}u_1 = P_1\frac{\mathrm{d}x}{\pi^{\alpha_1}}$. The ring P_1 is identical with the ring R_{α_1} of the quadratic sequence which connects $P[x]$ with R'.

With $\alpha_2 := v_R(g_1(u_1))$ and $u_2 := \frac{g_1(u_1)}{\pi^{\alpha_2}}$ we consider now the ring $P_1[u_2]$ where we have chosen a representative of the minimal polynomial of the residue class ξ_1 of u_1 with maximal value. Proceeding as above we construct a chain

$$P_0 \subset P_1 \subset P_2 \subset \cdots \subset P_i \subset \cdots \subset R'$$

of two-dimensional regular local rings P_i with separable algebraic extensions $\mathfrak{k}(P_i)/\mathfrak{k}(P_{i-1})$ of degree > 1 where $\Omega^1_{P_i/P} = P_i\mathrm{d}u_i = P_i\frac{\mathrm{d}x}{\pi^{\alpha_1+\cdots+\alpha_i}}$.

Since $\mathfrak{k}(R)/\mathfrak{k}(P)$ is a finitely generated field extension the algebraic closure of $\mathfrak{k}(P)$ in $\mathfrak{k}(R)$ has finite degree over $\mathfrak{k}(P)$. Therefore the above construction must end after finitely many steps. This happens when $\mathfrak{m}_R \cap P_n[u_{n+1}] = \pi P_n[u_{n+1}]$ and hence $R' = P_n[u_{n+1}]_{(\pi)}$. In particular we obtain that R' is essentially of finite type over P. Further the residue ξ_{n+1} of u_{n+1} in $\mathfrak{k}(R')$ is transcendental over $\mathfrak{k}(P_n)$ and

$$\Omega^1_{R'/P} = R'\mathrm{d}u_{n+1} = R'\frac{\mathrm{d}x}{\pi^{\alpha_1+\cdots+\alpha_{n+1}}}.$$

The quadratic sequence which connects $P[x]$ with R' is a refinement of the sequence constructed above: $P_i = R_{\alpha_1+\cdots+\alpha_i}$. Therefore $s = \alpha_1 + \cdots + \alpha_{n+1}$, and the assertion about $\Omega^1_{R'/P}$ is also proved. □

Remarks 2.2. (a) Under the assumptions of 2.1 the ring R is a localization of the integral closure of R' in K, but not each such localization needs to be smooth over P. Likewise not every discrete valuation ring R' of $k(x)$ which is smooth over P is dominated by a smooth discrete valuation ring R of K.

(b) Proposition 2.1 can be applied in the special case $K = k(x)$. Together with its proof it describes the discrete valuation rings of $k(x)$ which are essentially of finite type and smooth over P, and their modules of differentials. The proof shows how they can be constructed.

(c) The proof has shown that $\mathfrak{k}(R')$ is a rational function field of one variable over the algebraic closure of $\mathfrak{k}(P)$ in $\mathfrak{k}(R')$. This fact holds more generally, see Abhyankar [1] and Nagata [9].

3. Smooth discrete valuation rings in Fermat fields

In the Fermat field $K_m = \mathbf{Q}(x, y)$ we consider the set V_s defined in the introduction and the set V_s' of all discrete valuation rings R' with $Q(R') = \mathbf{Q}(x)$ which are essentially of finite type and smooth over $\mathbf{Z}$. Set $S := \mathbf{Z}[x, y]$ and $\tilde{S} := \mathbf{Z}[\tilde{x}, \tilde{y}]$ with $\tilde{x} := \frac{1}{x}$, $\tilde{y} := \frac{y}{x}$. Then Spec$S$ and Spec$\tilde{S}$ form an open affine covering of the projective Fermat scheme

$$X := \operatorname{Proj} \mathbf{Z}[X_0, X_1, X_2]/(X_1^m + X_2^m - X_0^m).$$

For $R \in V_s$ we have $S \subset R$ or $\tilde{S} \subset R$. We consider at the first case $S \subset R$. Since $\tilde{x}^m - \tilde{y}^m = 1$ the considerations in the case $\tilde{S} \subset R$ are similar, and it suffices to assume in this case that $v_R(\tilde{x}) > 0$.

If $\mathbf{Q} \subset R$, then R is the local ring at a point of the Fermat curve over $\mathbf{Q}$, that is $R = \mathbf{Q}[x, y]_{\mathfrak{m}}$ with a maximal ideal $\mathfrak{m}$ of $\mathbf{Q}[x, y]$. Then $\Omega^1_{R,\mathbf{Z}} = R\omega$ with ω as in (1.1) of the introduction. Therefore we have only to discuss the case that $\mathfrak{m}_R \cap \mathbf{Z} = (p)$ with a prime number p. Smoothness over $\mathbf{Z}$ then means that $\mathfrak{m}_R = pR$.

Assume that $p \nmid m$, and let $R' \in V_s'$ with $\mathfrak{m}_{R'} = pR'$ be given. Then

$$R'[y]/pR'[y] = \mathfrak{k}(R')[Y]/(Y^m + \xi^m - 1)$$

with the residue class ξ of x in $\mathfrak{k}(R')$. Since $Y^m + \xi^m - 1$ is a separable polynomial the ring $R'[y]/pR'[y]$ is a direct product of separable extension fields of $\mathfrak{k}(R')$. If $\mathfrak{m}_1, \ldots, \mathfrak{m}_r$ are the corresponding maximal ideals of $R'[y]$, then all $R'[y]_{\mathfrak{m}_i}$ belong to V_s, and all $R \in V_s$ with $p \in \mathfrak{m}_R$, $p \nmid m$ are gotten in this way. Using Proposition 2.1 we obtain

$$\Omega^1_{R/\mathbf{Z}} = R \otimes_{R'} \Omega^1_{R'/\mathbf{Z}} = R\frac{\mathrm{d}x}{p^s}$$

where s is the length of the quadratic sequence connecting $\mathbf{Z}_{(p)}[x]$ with R'.

It remains to study the $R \in V_s$ with $p \in \mathfrak{m}_R$, $p \mid m$. We denote by $V_s(p)$ the set of these R, and by v_p the p-adic valuation on $\mathbf{Q}$. Write $m = p^\nu m'$ with $p \nmid m'$. With $z := x^{m'} + y^{m'} - 1$, by the binomial theorem, the Fermat equation can be written in the following form

$$z^{p^\nu} + \sum_{i=1}^{p^\nu - 1} \binom{p^\nu}{i} z^{p^\nu - i}(1 - x^{m'})^i + ph_\nu(x) = 0 \tag{3.1}$$

where

$$h_\nu(x) := \frac{1}{p}[(x^{m'})^{p^\nu} + (1 - x^{m'})^{p^\nu} - 1].$$

This polynomial is divisible by $x^{m'}$ and $1 - x^{m'}$. If p is odd, then

$$h_\nu(x) = \frac{1}{p} \sum_{i=1}^{p^\nu - 1} \binom{p^\nu}{i} (-x^{m'})^i \tag{3.2}$$

and in case $p = 2$ we have

$$h_\nu(x) = (x^{m'})^{2^\nu} + \frac{1}{2} \sum_{i=1}^{2^\nu - 1} \binom{2^\nu}{i} (-x^{m'})^i. \tag{3.3}$$

Observe that not all coefficients of h_ν are divisible by p.

For $R \in V_s(p)$ and $S \subset R$ Eq. (3.1) shows $v_R(z) > 0$. But then $v_R(h_\nu(x)) \geq \nu$ because all summands other than $ph_\nu(x)$ have value $\geq \nu + 1$. Let $\mathfrak{p} := \mathfrak{m}_R \cap \mathbf{Z}[x]$, hence $p\mathbf{Z}[x] \subset \mathfrak{p}$. Since $h_\nu(x) \in \mathfrak{p}$ and $p \nmid h_\nu(x)$ we cannot have $\mathfrak{p} = p\mathbf{Z}[x]$. In particular $R' := \mathbf{Z}[x]_{(p)}$ is not dominated by any $R \in V_s(p)$. As $\mathfrak{p}$ is a maximal ideal of $\mathbf{Z}[x]$ it is of the form $\mathfrak{p} = (p, f)$ with a normed, modulo p irreducible polynomial $f \in \mathbf{Z}[x]$, and $R' := R \cap \mathbf{Q}(x)$ is one of the rings in V_s' which dominate $\mathbf{Z}[x]_{(p,f)}$.

We denote the reduction mod p of polynomials from $\mathbf{Z}[x]$ by a bar. Since $h_\nu \in (p, f)$ the polynomial $\bar{f}$ divides $\bar{h}_\nu$ in $\mathbf{F}_p[x]$. The polynomial x and the irreducible factors of $x^{m'} - 1 \in \mathbf{F}_p[x]$ certainly belong to these $\bar{f}$. So far we have shown

Proposition 3.1. *Let p be a prime number and $m = p^\nu m'$ with $\nu \geq 1$, $p \nmid m'$. For $R \in V_s(p)$ we have $v_R(h_\nu(x)) \geq \nu$ and R dominates one of the rings $\mathbf{Z}[x]_{(p,f)}$ where $f \in \mathbf{Z}[x]$ is normed, mod p irreducible, and where its reduction $\bar{f}$ divides $\bar{h}_\nu$.*

We consider now some properties of the polynomials $h_\nu(x)$.

Lemma 3.2. *We have $\bar{h}_\nu(x) = \bar{h}_1(x)^{p^{\nu-1}}$. For all $\nu \geq 1$ the polynomials $\bar{h}_\nu(x)$ have the same irreducible factors.*

Proof. The relation $v_p\left(\binom{p^\nu}{i}\right) = \nu - v_p(i)$ implies that $v_p\left(\binom{p^\nu}{i}\right) = 1$ if and only if $i = jp^{\nu-1}$ with some $j \in \{1, \ldots, p-1\}$. For odd p it follows from (3.2) that

$$\bar{h}_\nu(x) = \left[\sum_{j=1}^{p-1} a_j(-x^{m'})^j\right]^{p^{\nu-1}}$$

where a_j is the residue of $\frac{1}{p}\binom{p^\nu}{jp^{\nu-1}}$, hence $a_j = (-1)^{jp^{\nu-1}-1}\bar{j}^{-1}$ with the residue $\bar{j}$ of j. Therefore

$$\bar{h}_\nu(x) = \left[-\sum_{j=1}^{p-1} \bar{j}^{-1}(x^{m'})^j\right]^{p^{\nu-1}} = \bar{h}_1(x)^{p^{\nu-1}}.$$

For $p = 2$ it follows from (3.3) that

$$\bar{h}_\nu(x) = (x^{m'})^{2^\nu} + (-1)^{2^{\nu-1}-1}(-x^{m'})^{2^{\nu-1}} = (x^{m'})^{2^{\nu-1}}(x^{m'} - 1)^{2^{\nu-1}}.$$

In particular $\bar{h}_1(x) = x^{m'}(x^{m'} - 1)$, and the assertion follows also in this case. □

Examples 3.3. (a) $p = 2$. For the above $\bar{f}$ we have only to consider x and the irreducible factors of $x^{m'} - 1$ in $\mathbf{F}_2[x]$.

(b) $p = 3$. Again we have $\bar{h}_1(x) = x^{m'}(x^{m'} - 1)$ and only x and the irreducible factors of $x^{m'} - 1$ in $\mathbf{F}_3[x]$ have to be considered.

(c) $p = 5$. Here $\bar{h}_1(x) = x^{m'}(x^{m'} - 1)((x^{m'})^2 - x^{m'} + 1)$ and $x^2 - x + 1$ is in the case $m' = 1$ an irreducible factor of $\bar{h}_1(x)$.

(d) $p = 7$. Here $\bar{h}_1(x) = x^{m'}(x^{m'} - 1)(x^{m'} - 3)^2(x^{m'} - 5)^2$.

Remarks 3.4. (a) If $m = p \geq 5$ with a prime number p, then the polynomial $h_1(-x) = \frac{1}{p}\sum_{i=1}^{p-1}\binom{p}{i}x^i$ can be written in the form

$$h_1(-x) = x(x + 1)(x^2 + x + 1)C_p(x)$$

in the case $p \equiv -1 \bmod 6$, and in the form

$$h_1(-x) = x(x + 1)(x^2 + x + 1)^2C_p(x)$$

in the case $p \equiv 1 \bmod 6$. The $C_p(x)$ are called *Cauchy polynomials*. It is unknown whether they are always irreducible, see Ribenboim [10] for the history of these polynomials.

(b) Each $\mathfrak{m} \in \operatorname{Max} S$ with $p \in \mathfrak{m}$ contains z and a polynomial $f \in \mathbf{Z}[x]$ which is irreducible mod p. If ξ is residue of x in $\mathbf{F}_p[x]/(f)$, then $S/(p, f, z) = \mathbf{F}_p[\xi][Y]/(Y^{m'} + \xi^{m'} - 1)$ is a direct product of fields, and $\mathfrak{m}$ corresponds to

one of the factors in this product. The maximal ideal of $S_{\mathfrak{m}}$ is generated by p, z and f. Eq. (3.1) shows that $S_{\mathfrak{m}}$ is a regular local ring if and only if $\bar{f} \nmid \bar{h}_\nu$, because otherwise (3.1) gives a quadratic relation among p, z and f. The condition $\bar{f} \mid \bar{h}_\nu$ is therefore equivalent with $\mathfrak{m}$ being a singularity of the Fermat scheme X. By 3.1 the $R \in V_s(p)$ dominate local rings of singularities of X. For a detailed discussion of these singularities in the case $m = p$, see Maeda [7]. Notice also the later Remark 3.12.

Lemma 3.5. *Assume that $R' \in V_s'$ dominates $\mathbf{Z}[x]_{(p,x)}$, and set*

$$v_{R'}(x) =: \alpha, \qquad v_{R'}(h_\nu(x)) =: \beta.$$

If $p \neq 2$, then

$$\beta = m'\alpha + \nu - 1 \geq \nu.$$

This holds true also for $p = 2$ when $m' > 1$ or $\alpha > 1$. If $p = 2$, $m'\alpha = 1$ we still have $\beta \geq \nu$.

Proof. If $p \neq 2$ the terms in formula (3.2) for $h_\nu(x)$ have values

$$\nu - 1 - v_p(i) + m'\alpha i \quad (i = 1, \ldots, p^\nu - 1).$$

For $i = 1$ we obtain the uniquely determined smallest value. For $p = 2$, $\nu = 1$ obviously $\beta = m'\alpha$. If $\nu > 1$, then the values of the terms in formula (3.3) for $h_\nu(x)$ are $2^\nu m'\alpha$ and $\nu - 1 - v_2(i) + m'\alpha i$ $(i = 1, \ldots, 2^\nu - 1)$. We obtain the smallest value for $i = 1$, and it is unique, when $m'\alpha > 1$. □

Now we write the Fermat equation in the following form

$$(y^{m'})^{p^\nu} + \sum_{i=1}^{p^\nu} \binom{p^\nu}{i} (x^{m'} - 1)^i = 0. \tag{3.4}$$

Lemma 3.6. *For $R \in V_s(p)$ we have*

(a) *$v_R(x^{m'} - 1) > 0$ if and only if $v_R(y) > 0$.*
(b) *If $p \neq 2$ and one of the equivalent conditions of* (a) *is satisfied, then*

$$v_R(x^{m'} - 1) = m v_R(y) - \nu.$$

(c) *This holds true also for $p = 2$ when $v_R(x^{m'} - 1) > 1$.*

Proof. (a) Follows directly from (3.4). Under the assumptions of (b) or (c) the term for $i = 1$ in formula (3.4) has the unique minimal value, and the formula of (b) follows. □

We shall use the lemma as follows. If $R \in V_s(p)$ dominates a local ring $\mathbf{Z}[x]_{(p,f)}$ with $\bar{f} \mid x^{m'} - 1$, then R also dominates $\mathbf{Z}[y]_{(p,y)} \subset \mathbf{Q}(y)$. Thus by exchanging the roles of x and y the investigation of R can be reduced to the case $f = x$.

We show another property of the rings $R \in V_s(p)$, a necessary condition for their construction in the following theorem. For $f = x$ however, due to 3.5, it is automatically satisfied.

Lemma 3.7. *Assume $p \neq 2$. For each $R \in V_s(p)$ which dominates $\mathbf{Z}[x]_{(p,f)}$ with $\bar{f} \nmid x^{m'} - 1$ we have $\beta := v_R(h_\nu(x)) = v_R(z) + \nu - 1 \geq \nu$, hence $v_R(z) = \beta - \nu + 1$.*

Proof. Consider the value of the terms in Eq. (3.1). If $p \neq 2$ the term with $i = p^\nu - 1$ has the uniquely determined lowest value $\nu + v_R(z)$ among all terms different from $ph_\nu(x)$. Therefore $\nu + v_R(z) = \beta + 1$. □

We now turn to the construction of rings from $V_s(p)$. The case $p = 2$ has to be treated separately.

Theorem 3.8. *Assume $p \neq 2$ and let $R' \in V_s'$ dominate a ring $\mathbf{Z}[x]_{(p,f)}$ where $f \in \mathbf{Z}[x]$ is normed,* mod p *irreducible and $\bar{f}$ does not divide $x^{m'} - 1$ in $\mathbf{F}_p[x]$. Assume that $\beta := v_{R'}(h_\nu(x)) \geq \nu$, let ξ be the residue of x in $\mathbf{Z}[x]/(p, f)$ and let r be the number of irreducible factors of the polynomial $Y^{m'} - (1 - \xi^{m'}) \in \mathfrak{k}(R')[Y]$. Then $R'[w]$ with $w := \frac{z}{p^{\beta-\nu+1}}$ is the only discrete valuation ring in $\mathbf{Q}(x, y^{m'})$ lying over R' and being smooth over $\mathbf{Z}$. In K_m there*

are exactly r rings $R \in V_s(p)$ which dominate R', namely the localizations of $R'[w, y]$ with respect to its maximal ideals. For their differential modules we have

$$\Omega^1_{R/\mathbf{Z}} = R \otimes_{R'} \Omega^1_{R'/\mathbf{Z}} = R\frac{\mathrm{d}x}{p^s}$$

where s is the length of the quadratic sequence connecting $\mathbf{Z}_{(p)}[x]$ with R', $s \geq v_{R'}(f)$.

Proof. Dividing Eq. (3.1) by $p^{\beta+1}$ we obtain

$$\sum_{i=0}^{p^\nu-1} \binom{p^\nu}{i} p^{(p^\nu-i)(\beta-\nu+1)-\beta-1} w^{p^\nu-i}(1-x^{m'})^i + \frac{h_\nu(x)}{p^\beta} = 0. \tag{3.5}$$

We consider at first the exponent of the term for $i = 0$

$$p^\nu(\beta-\nu+1)-\beta-1 = (p^\nu-1)\left(\beta-\nu+1-\frac{\nu}{p^\nu-1}\right).$$

If $p \neq 2$, since $\beta \geq \nu$, this exponent is > 0. Moreover for $i = 1, \ldots, p^\nu - 1$

$$v_{R'}\left(\binom{p^\nu}{i} p^{(p^\nu-i)(\beta-\nu+1)-\beta-1}\right) = (p^\nu-i-1)(\beta-\nu+1) - v_{R'}(i) \geq 0$$

and this value vanishes only for $i = p^\nu - 1$. Therefore we have

$$R'[w]/pR'[w] = \mathfrak{k}(R')[W]/((1-\xi^{m'})^{p^\nu-1}W + \eta)$$

with the residue η of $\frac{h_\nu(x)}{p^\beta}$ in $\mathfrak{k}(R')$. From $\bar{f} \nmid x^{m'} - 1$ we obtain that $1 - \xi^{m'} \neq 0$. Therefore $R'[w]/pR'[w]$ is a field, isomorphic to $\mathfrak{k}(R')$, hence $pR'[w] \in \operatorname{Max} R'[w]$. For $\mathfrak{P} \in \operatorname{Spec} R'[w]$ with $p \notin \mathfrak{P}$ we have $\mathfrak{P} \cap R' = (0)$, therefore $\mathbf{Q}(x)[z] = \mathbf{Q}(x, y^{m'}) \subset R'[w]_{\mathfrak{P}}$, and hence $\mathfrak{P} = (0)$. It follows that $R_0 := R'[w]$ is a discrete valuation ring of $\mathbf{Q}(x, y^{m'})$ which is smooth over $\mathbf{Z}$.

We show that R_0 is the only ring of this kind which dominates R'. With $u := \frac{1}{w}$ we obtain from (3.5) the equation

$$\frac{p^\beta}{h_\nu(x)} \sum_{i=0}^{p^\nu-2} \binom{p^\nu}{i} p^{(p^\nu-i)(\beta-\nu+1)-\beta-1}(1-x^{m'})^i u^i + (\theta+u)u^{p^\nu-1} = 0 \tag{3.6}$$

with $\theta := \frac{p^\beta}{h_\nu(x)}(1-x^{m'})^{p^\nu-1}$. This is an irreducible equation of integral dependence for u over R'. It follows that $R'[u]/pR'[u] = \mathfrak{k}(R')[U]/(U^{p^\nu-1}(U+\bar{\theta}))$ with the residue $\bar{\theta}$ of θ in $\mathfrak{k}(R')$. There are exactly two maximal ideals in $R'[u]$ lying over pR', namely $\mathfrak{m} := (p, u+\theta)$ and $\mathfrak{m}' := (p, u)$, and $R'[u]_{\mathfrak{m}} = R_0$ is the ring which was constructed above.

Assume there were another discrete valuation ring R_1 of $\mathbf{Q}(x, y^{m'})$ which dominates R' and is smooth over $\mathbf{Z}$. Then we would have $\mathfrak{m}_{R_1} \cap R'[u] = \mathfrak{m}'$ and $v_{R_1}(u) > 0$. Consider the value of the terms in Eq. (3.6). These are the numbers

$$\begin{aligned} &p^\nu(\beta-\nu+1)-\beta-1 = (p^\nu-1)(\beta-\nu+1)-\nu \quad \text{for } i = 0\\ &(p^\nu-i-1)(\beta-\nu+1) - v_{R_1}(i) + i\,v_{R_1}(u) \quad \text{for } i = 1, \ldots, p^\nu-2 \end{aligned}$$

and

$$(p^\nu-1)v_{R_1}(u).$$

If $v_{R_1}(u) \geq \beta-\nu+1$, then writing the numbers for $i = 1, \ldots, p^\nu-2$ in the form

$$(p^\nu-1)(\beta-\nu+1) - v_{R_1}(i) + i(v_{R_1}(u) - \beta + \nu - 1)$$

we notice that $(p^\nu-1)(\beta-\nu+1)-\nu$ is the uniquely determined smallest of the above numbers. If $v_{R_1}(u) < \beta-\nu+1$, then we write the numbers in the form

$$(p^\nu-i-1)(\beta-\nu+1-v_{R_1}(u)) - v_{R_1}(i) + (p^\nu-1)v_{R_1}(u)$$

and observe that in this case $(p^\nu-1)v_{R_1}(u)$ is the unique minimal one. In Eq. (3.6) there was a unique term of minimal value. This contradiction proves the uniqueness statement of the theorem.

For each $R \in V_s(p)$ which dominates R' we must have $R \cap \mathbf{Q}(x, y^{m'}) = R_0$. Since $x^{m'} - 1$ is a unit of R' and $z = x^{m'} + y^{m'} - 1$ a non-unit the residue of $y^{m'}$ in $\mathfrak{k}(R')$ is $1 - \xi^{m'}$. As $p \nmid m'$ the ring

$$R_0[y]/pR_0[y] = \mathfrak{k}(R_0)[Y]/(Y^{m'} - (1 - \xi^{m'}))$$

is a direct product of r finite separable extension fields of $\mathfrak{k}(R_0)$. Therefore there are exactly r rings $R \in V_s(p)$ which dominate R', and $\mathfrak{k}(R)$ is separable over $\mathfrak{k}(R_0) = \mathfrak{k}(R')$. It follows that

$$\Omega^1_{R/\mathbf{Z}} = R \otimes_{R'} \Omega^1_{R'/\mathbf{Z}}.$$

The last statement of the theorem follows from 2.1. □

In the case $p = 2$ we have to consider only the $R' \in V'_s$ which dominate $\mathbf{Z}[x]_{(2,x)}$. Then $v_{R'}(x) > 0$.

Theorem 3.9. *Let $p = 2$. For each $R' \in V'_s$ which dominates $\mathbf{Z}[x]_{(2,x)}$ there exist exactly two smooth discrete valuation rings with quotient field $\mathbf{Q}(x, y^{m'})$ which dominate R'. They are the localizations of $R'[w]$ with $w := \frac{y^{m'}-1}{2}$ at the maximal ideals $\mathfrak{m} := (2, w+1)$ and $\mathfrak{m}' := (2, w)$. If r is the number of irreducible factors of the polynomial $Y^{m'} - 1$ in $\mathfrak{k}(R')[Y]$, then $R'[w]_\mathfrak{m}$ and $R'[w]_{\mathfrak{m}'}$ are dominated by exactly r elements $R \in V_s(2)$, the localizations of $R'[w]_\mathfrak{m}[y]$ resp. $R'[w]_{\mathfrak{m}'}[y]$ at their maximal ideals. Moreover*

$$\Omega^1_{R/\mathbf{Z}} = R \otimes_{R'} \Omega^1_{R'/\mathbf{Z}} = R\frac{\mathrm{d}x}{2^s}$$

where s is the length of the quadratic sequence which connects $\mathbf{Z}_{(2)}[x]$ with R', $s \geq v_{R'}(x)$.

Proof. Dividing the Fermat equation

$$\sum_{i=1}^{2^\nu} \binom{2^\nu}{i} (y^{m'} - 1)^i + x^m = 0$$

by $2^{\nu+1}$ we obtain with $\alpha := v_{R'}(x)$ and $\epsilon := \frac{x}{2^\alpha}$ an equation

$$\sum_{i=1}^{2^\nu} b_i w^i + 2^{m\alpha-\nu-1}\epsilon^m = 0$$

with $b^i \in \mathbf{Z}$ $(i = 1, \ldots, 2^\nu)$, where $v_2(b_i) = i - v_2(i) - 1$. Here $v_2(b_i) = 0$ for $i = 1$ and $i = 2$, otherwise $v_2(b_i) > 0$. It follows that

$$R'[w]/2R'[w] = \mathfrak{k}(R')[W]/(W(W+1)).$$

Therefore $R'[w]$ has only the maximal ideals $\mathfrak{m}$ and $\mathfrak{m}'$, and $R'[w]_\mathfrak{m}$ as well as $R'[w]_{\mathfrak{m}'}$ are smooth discrete valuation rings with quotient field $\mathbf{Q}(x, y^{m'})$ and residue field $\mathfrak{k}(R')$. If R_0 is an arbitrary smooth discrete valuation ring with quotient field $\mathbf{Q}(x, y^m)$ lying over R', then the Fermat equation shows that $v_{R_0}(y^{m'} - 1) > 0$, hence $w \in R_0$, and R_0 is one of the two localizations of $R'[w]$ mentioned above.

The same argument as in the proof of Theorem 3.8 shows that each of the localizations is dominated by exactly r rings $R \in V_s(2)$, and they have a residue field which is separably algebraic over $\mathfrak{k}(R')$. For any such R the assertion about differential modules then also follows. □

It remains to consider the $R \in V_s(p)$ with $\tilde{S} \subset R$, where it is enough to look at the $R' \in V'_s$ with $v_{R'}(\tilde{x}) > 0$. For $p \neq 2$ the equation $\tilde{x}^m - \tilde{y}^m = 1$ can be written as follows

$$(\tilde{x}^{m'})^{p^\nu} - \sum_{i=1}^{p^\nu} (-1)^i \binom{p^\nu}{i} (\tilde{y}^{m'} + 1)^i = 0. \tag{3.7}$$

Theorem 3.10. *Let $R' \in V_s'$ with $v_{R'}(\tilde{x}) =: \alpha > 0$ be given. If $p \neq 2$, then $R_0 := R'[\tilde{v}]$ with $\tilde{v} := \frac{\tilde{y}^{m'}+1}{p^{m\alpha-\nu}}$ is the only smooth discrete valuation ring which dominates R' and has quotient field $\mathbf{Q}(\tilde{x}, \tilde{y}^{m'}) = \mathbf{Q}(x, y^{m'})$. If r is the number of irreducible factors of the polynomial $Y^{m'} + 1 \in \mathfrak{k}(R')[Y]$, then there are exactly r elements $R \in V_s(p)$ which dominate R_0. They are the localizations of $R_0[\tilde{y}]$ at its maximal ideals. Moreover*

$$\Omega^1_{R/\mathbf{Z}} = R \otimes_{R'} \Omega^1_{R'/\mathbf{Z}} = R\frac{\mathrm{d}\tilde{x}}{p^s}$$

where s is the length of the quadratic sequence connecting $\mathbf{Z}_{(p)}[\tilde{x}]$ with R', $s \geq v_{R'}(\tilde{x})$.

Proof. Dividing (3.7) by $p^{m\alpha}$ we obtain with $\tilde{u} := (\frac{\tilde{x}}{p^\alpha})^{m'}$ the equation

$$\tilde{u}^{p^\nu} - \sum_{i=1}^{p^\nu} (-1)^i \binom{p^\nu}{i} p^{i(m\alpha-\nu)-m\alpha} \tilde{v}^i = 0.$$

Here

$$v_p\left(\binom{p^\nu}{i} p^{i(m\alpha-\nu)-m\alpha}\right) = (i-1)(m\alpha-\nu) - v_p(i) \geq 0$$

for $i = 1, \ldots, p^\nu$, and the value is 0 only for $i = 1$. With an analogous argument as in the proof of Theorem 3.8 it follows that R_0 is a smooth discrete valuation ring with $\mathfrak{k}(R_0) = \mathfrak{k}(R')$ which is dominated by r elements $R \in V_s(p)$. If $R \in V(p)$ is an arbitrary ring which dominates R', then it follows from (3.7) that $v_R(\tilde{y}^{m'}+1) = m\alpha - \nu$. Therefore $R_0 \subset R$, hence $R_0 = R \cap \mathbf{Q}(\tilde{x}, \tilde{y}^{m'})$ is the only smooth discrete valuation ring of $\mathbf{Q}(\tilde{x}, \tilde{y}^{m'})$ which dominates R'. The assertion about differential modules follows as earlier. □

The proof shows that in the special case $f = x$ Theorem 3.8 has a shorter proof than the one given there.

Theorem 3.11. *Let $m = 2^\nu m'$ with $\nu \geq 1$ and $2 \nmid m'$. Then no $R \in V_s(2)$ exists with $v_R(\tilde{x}) > 0$.*

Proof. The equation $\tilde{x}^m - \tilde{y}^m = 1$ can be written in the following form

$$\tilde{x}^m - \sum_{i=1}^{2^\nu} \binom{2^\nu}{i} (\tilde{y}^{m'} - 1)^i - 2 = 0. \tag{3.8}$$

For $i \neq 2^\nu$ the binomial coefficients are divisible by 2. If $v_R(\tilde{x}) > 0$ for some $R \in V_s(2)$, then $v_R(\tilde{y}^{m'} - 1) > 0$. All terms other than -2 in Eq. (3.8) would have value > 1, a contradiction. □

Remark 3.12. In the case $p \neq 2$ each $\mathfrak{M} \in \operatorname{Max} \tilde{S}$ which contains p and $\tilde{x}$ is a singularity of the Fermat scheme X, since Eq. (3.7) contains only quadratic terms and terms of higher order in $p, \tilde{x}$ and $\tilde{y}^{m'} - 1$. However in the case $p = 2$ Eq. (3.8) shows that all $\mathfrak{M} \in \operatorname{Max} \tilde{S}$ with $2, \tilde{x} \in \mathfrak{M}$ are regular points of X. It follows easily from 3.8–3.10 that the local ring of each singularity of X is dominated by some $R \in V_s$.

4. Differentials of Fermat fields

We shall study now the abelian groups mentioned in the introduction. Besides the differential $\omega := \frac{\mathrm{d}x}{y^{m-1}} = -\frac{\mathrm{d}y}{x^{m-1}} \in \Omega^1_{K_m/\mathbf{Q}}$ we have also to use $\tilde{\omega} := \frac{\mathrm{d}\bar{x}}{\bar{y}^{m-1}} = \frac{\mathrm{d}\bar{y}}{\bar{x}^{m-1}}$. Here $\tilde{\omega} = -x^{m-3}\omega$ and $\omega = -\tilde{x}^{m-3}\tilde{\omega}$. By [5], Proposition 2.1 we have

$$\frac{1}{\mathfrak{d}_1(R/\mathbf{Z})}[R, \mathrm{d}R]^1 = \omega^1_{R/\mathbf{Z}} \tag{4.1}$$

for all $R \in V$ where $\omega^1_{R/\mathbf{Z}}$ denotes the module of regular differentials of $R/\mathbf{Z}$.

Theorem 4.1. *For each prime $p \mid m$ we have $\frac{\omega}{p} \in D^1(\frac{K_m}{\mathfrak{d}})$ and $\frac{\tilde{\omega}}{p} \in D^1(\frac{K_m}{\mathfrak{d}})$. In particular $D^1(\frac{K_m}{\mathfrak{d}})/D^1(K_m)$ and $D^1_s(K_m)/D^1(K_m)$ are nonvanishing groups.*

Proof. We must show that $\frac{\omega}{p} \in \omega^1_{R/\mathbf{Z}}$ for all $R \in V$. Assume at first that $S \subset R$ and without restriction that y is a unit of R. Then we have to prove that $\frac{\mathrm{d}x}{p} \in \omega^1_{R/\mathbf{Z}}$. If $p \notin \mathfrak{m}_R$ this is clear, so let $p \in \mathfrak{m}_R$. If $\mathfrak{p} := \mathfrak{m}_R \cap S$ is a prime ideal of height 1 of S, then $R = S_{\mathfrak{p}}$ since S is normal. Then $\mathfrak{d}_1(R/\mathbf{Z}) = \mathfrak{p}^\nu R$ with $\nu \geq 1$, and the assertion is also true.

Assume now that $\mathfrak{m}_R \cap \mathbf{Z}[x] = (p, f)$ is a maximal ideal of $\mathbf{Z}[x]$ with a polynomial $f \in \mathbf{Z}[x]$ which is modulo p irreducible and separable. Since $f'(x)$ is a unit of R we may replace $\frac{\mathrm{d}x}{p}$ by $\frac{\mathrm{d}f}{p}$. Set $u := \frac{p^{v_R(f)}}{f^e}$ with the ramification index $e := v_R(p)$. Then u is a unit of R, and from the equation $f^e \mathrm{d}u + ef^{e-1}u\mathrm{d}f = 0$ we obtain in $[R, \mathrm{d}R]^1$ the equation $f\mathrm{d}u + eu\mathrm{d}f = 0$, hence

$$v_R(\mathrm{d}f) = v_R(f) + v_R(\mathrm{d}u) - v_R(e).$$

(a) If $p \nmid e$, then $v_R(\mathfrak{d}_1(R/\mathbf{Z})) = e - 1$ and $v_R(\mathrm{d}f) = v_r(f) + v_R(\mathrm{d}u) \geq 1$, hence $v_R(\frac{\mathrm{d}f}{p}) = v_R(\mathrm{d}f) - e \geq 1 - e = -v_R(\mathfrak{d}_1(R/\mathbf{Z}))$ from which $\frac{\mathrm{d}f}{p} \in \omega^1_{R/\mathbf{Z}}$ follows.

(b) If $p \mid e$, then $v_R(\mathfrak{d}_1(R/\mathbf{Z})) \geq e$ and $v_R(\frac{\mathrm{d}f}{p}) \geq -e \geq -v_R(\mathfrak{d}_1(R/\mathbf{Z}))$, from which the desired assertion also follows.

In the case $\tilde{S} \subset R$ we have analogously $\frac{\tilde{\omega}}{p} \in \omega^1_{R/\mathbf{Z}}$. Since $\omega = -\tilde{x}^{m-3}\tilde{\omega}$ and $\tilde{x} \in R$ we obtain also here that $\frac{\omega}{p} \in \omega^1_{R/\mathbf{Z}}$. This shows that $\frac{\omega}{p} \in D^1(\frac{K_m}{\mathfrak{d}})$. By symmetry $\frac{\tilde{\omega}}{p} \in D^1(\frac{K_m}{\mathfrak{d}})$.
The last statement of the theorem follows from formula (1.1) of the introduction. □

Remark 4.2. If $Y/\mathbf{Z}$ is a complete regular model of K_m, then by Berndt [2], Section 7

$$D^1\left(\frac{K_m}{\mathfrak{d}}\right) = H^0(Y, \omega^1_{Y/\mathbf{Z}})$$

with the sheaf $\omega^1_{Y/\mathbf{Z}}$ of regular differentials of $Y/\mathbf{Z}$. Here

$$H^0(Y, \omega^1_{Y/\mathbf{Z}}) = \bigcap \omega^1_{R/\mathbf{Z}} \tag{4.2}$$

where the intersection is to be extended over all local rings R of dimension 1 of Y. If these rings are known explicitly, i.e. given by generators and relations, then one can try to compute $D^1(\frac{K_m}{\mathfrak{d}})$ by formula (4.2). In an example ($m = 4$) this will be carried out later.

Set $M := \{1, m, m^2, \ldots\}$. Then $X_M := \operatorname{Spec} S_M \cup \operatorname{Spec} \tilde{S}_M$ is a projective model of K_m over $\mathbf{Z}_M$. Since locally x or y is a unit in S_M we have

$$\Omega^1_{S_M/\mathbf{Z}_M} = S_M\mathrm{d}X \oplus S_M\mathrm{d}Y/\langle mx^{m-1}\mathrm{d}X + my^{m-1}\mathrm{d}Y\rangle = S_M\omega$$

and similarly

$$\Omega^1_{\tilde{S}_M/\mathbf{Z}_M} = \tilde{S}_M\tilde{\omega} = \tilde{S}_M x^{m-3}\omega.$$

It follows that X_M is a smooth model of K_m over $\mathbf{Z}_M$. Setting $V_s(m) := \{R \in V_s | m \in \mathfrak{m}_R\}$ one finds easily that

$$\bigcap_{R \in V_s \setminus V_s(m)} \Omega^1_{R/\mathbf{Z}_M} = \left(\bigoplus_{i+k \leq m-3} \mathbf{Z}_M x^i y^k\right)\omega.$$

We conclude

Lemma 4.3. $D^1_s(K_m) = (\bigoplus_{i+k\leq m-3} \mathbf{Z}_M x^i y^k)\omega \cap \bigcap_{p|m} \bigcap_{R\in V_s(p)} \Omega^1_{R/\mathbf{Z}}$.

Theorem 4.4. *We have*

$$D^1_s(K_m) \subset \frac{1}{m^{(m-3)(m-1)}}\left(\bigoplus_{i+k\leq m-3} \mathbf{Z}x^i y^k\right)\frac{\omega}{m}.$$

In particular $D^1_s(K_m)$ is a free abelian group of rank $g := \binom{m-1}{2}$, and $D^1_s(K_m)/D^1(\frac{K_m}{\mathfrak{d}})$ as well as $D^1_s(K_m)/D^1(K_m)$ are finite abelian groups.

Proof. For a prime number $p \mid m$ write $m = p^{\nu}m'$ with $p \nmid m'$. If $p \neq 2$, then by Theorem 3.8 all $R \in V_s(p)$ which dominate $R' := \mathbf{Z}[\frac{x}{p}]_{(p)}$ contain also the ring

$$R'\left[\frac{z}{p}, y\right] = R'\left[\frac{y^{m'}-1}{p}, y\right]$$

where $z := x^{m'} + y^{m'} - 1$. Then $v_R(y^{m'} - 1) = m - \nu$ by 3.6(b).

If $p = 2$, then all $R \in V_s(2)$ which dominate $R' := \mathbf{Z}[\frac{x}{2}]_{(2)}$ contain one of the rings $R'[w]_{\mathfrak{m}}$ or $R'[w]_{\mathfrak{m}'}$ where $w := \frac{y^{m'}-1}{2}$ and $\mathfrak{m} = (2, w)$, $\mathfrak{m}' = (2, w + 1)$. In the first case we have again $v_R(y^{m'} - 1) = m - \nu$ by 3.6(c). We choose R in the case $p = 2$ so that this formula holds.

In both cases, by 3.8 and 3.9, we can choose R so that $y - 1 \in \mathfrak{m}_R$. Since $Y^{m'} - 1 \in \mathbf{F}_p[Y]$ is separable we then have $v_R(y - 1) = v_R(y^{m'} - 1)$. In any case we can find R so that $v_R(y - 1) = m - \nu$. Since $\Omega^1_{R'/\mathbf{Z}} = R'\frac{\omega}{p}$ we have $\Omega^1_{R/\mathbf{Z}} = R\frac{\omega}{p}$.

Set $u := \frac{x}{p}$ and $v := \frac{y-1}{p^{m-\nu}}$. Dividing the equation $x^m + \sum_{i=1}^{m}\binom{m}{i}(y-1)^i = 0$ by p^m we obtain

$$u^m + m'v + \sum_{i=2}^{m}\binom{m}{i}p^{i(m-\nu)-m}v^i = 0.$$

Here

$$v_p\left(\binom{m}{i}p^{i(m-\nu)-m}\right) = \nu - v_p(i) + i(m-\nu) - m = (i-1)(m-\nu) - v_p(i) > 0.$$

Denoting residue classes in $\mathfrak{k}(R)$ by a bar we obtain in $\mathfrak{k}(R)$ the equation $\bar{u}^m + \bar{m}'\bar{v} = 0$.

Let a differential $r\frac{\omega}{m} \in D^1_s(K_m)$ be given. By Lemma 4.3 we can write r in the form

$$r = \sum_{i+k\leq m-3} z_{ik}x^i(y-1)^k \quad (z_{ik} \in \mathbf{Z}_M).$$

Since $r\frac{\omega}{m} \in \Omega^1_{R/\mathbf{Z}} = R\frac{\omega}{p}$ we have $r\frac{p}{m} \in R$. Write

$$r\frac{p}{m} = \sum_{i+k\leq m-3}\frac{z_{ik}}{m'}\cdot p^{i+(m-\nu)k-\nu+1}u^iv^k$$

and set $\mu := \operatorname{Min}\{v_p(z_{ik}) + i + (m-\nu)k - \nu + 1 \mid i + k \leq m - 3\}$. Then

$$r\frac{p}{m} = p^{\mu}\sum_{i+k\leq m-3}a_{ik}u^iv^k \quad \text{with } a_{ik} \in \mathbf{Z}_M \cap R$$

where at least one a_{ik} is a unit of R. Using the relation $\bar{u}^m + \bar{m}'\bar{v} = 0$ the reduction of the sum modulo p leads to the expression

$$\sum_{i+k\leq m-3}(-1)^k\frac{\bar{a}_{ik}}{(\bar{m}')^k}\bar{u}^{i+mk} \in \mathbf{F}_p[\bar{u}].$$

Since the exponents $i + mk$ are mutually distinct and $\bar{u}$ is transcendental over $\mathbf{F}_p$ this expression does not vanish. From $r\frac{p}{m} \in R$ follows $\mu = v_R(r\frac{p}{m}) \geq 0$, hence

$$v_p(z_{ik}) + i + (m-\nu)k - \nu + 1 \geq 0$$

for all (i, k). Thus

$$v_p(z_{ik}) \geq -i - (m-\nu)k + \nu - 1 \geq -(m-3)(m-\nu-1) + \nu - 1 \geq -(m-3)(m-1)$$

and the desired estimate

$$D^1_s(K_m) \subset \frac{1}{m^{(m-3)(m-1)}}\left(\bigoplus_{i+k\leq m-3}\mathbf{Z}x^iy^k\right)\frac{\omega}{m}$$

follows. Since $D^1_s(K_m)$ contains the free abelian group $D^1(K_m)$ of rank g it is also free of this rank. □

Corollary 4.5. $D_s^1(K_3) = D^1(\frac{K_3}{\mathfrak{d}}) = \mathbf{Z}\frac{\omega}{3}$ *and* $D_s^1(K_3)/D^1(K_3) = \mathbf{Z}_3$.

Proposition 4.6. *Let p be a prime number with $p \mid m$. Then $\frac{\omega}{p^2} \notin D_s^1(K_m)$ and hence also $\frac{\omega}{p^2} \notin D^1(\frac{K_m}{\mathfrak{d}})$. If m is not squarefree, then*

$$D^1\left(\frac{K_m}{\mathfrak{d}}\right) \neq \left(\bigoplus_{i+k\leq m-3} \mathbf{Z}x^i y^k\right)\frac{\omega}{m}$$

and $D^1(\frac{K_m}{\mathfrak{d}})/D^1(K_m)$ is a proper quotient of $(\mathbf{Z}_m)^g$.

Proof. By 3.8 and 3.9 we can choose an $R \in V_s(p)$ which dominates $\mathbf{Z}[\frac{x}{p}]_{(p)}$. Then $\Omega^1_{R/\mathbf{Z}} = R\frac{\omega}{p}$, hence $\frac{\omega}{p^2} \notin \Omega^1_{R/\mathbf{Z}}$ and therefore $\frac{\omega}{p^2} \notin D_s^1(K_m)$. The remaining statements of the proposition are obvious. □

Proposition 4.7. (a) *If m_0 is the squarefree kernel of m, then $\frac{\omega}{m_0} \in D_s^1(K_m)$ and $\frac{\tilde{\omega}}{m_0} \in D_s^1(K_m)$.*
(b) *If m is squarefree ($m = m_0$) and $m > 3$, then for any prime p with $p \mid m$ and $m' := \frac{m}{p}$*

$$\frac{x^{m'} + y^{m'} - 1}{p}\frac{\omega}{m} \in D_s^1(K_m) \setminus D^1\left(\frac{K_m}{\mathfrak{d}}\right).$$

In the case $p = 3$ we have the stronger assertion

$$\frac{x^{m'} + y^{m'} - 1}{3^{m'}}\frac{\omega}{m} \in D_s^1(K_m) \setminus D^1\left(\frac{K_m}{\mathfrak{d}}\right).$$

(c) *If $m = p^\nu$ with a prime number p, then*

$$\left[\bigoplus_{i+k\leq m-3} \mathbf{Z}x^i\left(\frac{x+y-1}{p}\right)^k\right]\frac{\omega}{p} \subset D_s^1(K_m).$$

Proof. (a) By 4.1 we have $\frac{\omega}{p} \in \Omega^1_{R/\mathbf{Z}}$ for each prime $p \mid m$ and each $R \in V_s$, hence $\frac{\omega}{m_0} \in D_s^1(K_m)$. Similarly for $\tilde{\omega}$.

(b) By 3.8 respectively 3.9 we have $\frac{x^{m'}+y^{m'}-1}{p}\frac{\omega}{m} \in \Omega^1_{R/\mathbf{Z}}$ for each $R \in V_s(p)$ with $S \subset R$. If $R \in V_s(p)$ and $v_R(\tilde{x}) > 0$, then

$$\frac{x^{m'} + y^{m'} - 1}{p}\frac{\omega}{m} = \frac{\tilde{x}^{m'} - \tilde{y}^{m'} - 1}{p}\tilde{x}^{m-m'-3}\frac{\tilde{\omega}}{m}$$

is in the case $m - m' - 3 \geq 0$ an element of $\Omega^1_{R/\mathbf{Z}}$. For $m > 3$ this is certainly the case.

If $p = 3$ and $R \in V_s(3)$ with $S \subset R$ is given, then $x \in \mathfrak{m}_R$ or $y \in \mathfrak{m}_R$ by 3.3(b) and 3.6(a). Assume without restriction that $x \in \mathfrak{m}_R$. Then by 3.5 and 3.7 we have $v_R(z) = m'v_R(x) \geq m'$, hence $\frac{x^{m'}+y^{m'}-1}{3^{m'}} \in R$. In the case $v_R(\tilde{x}) > 0$ we have $v_R(\tilde{y}^{m'} + 1) \geq mv_R(\tilde{x}) - 1 \geq m'$ by 3.10, and we can argue as above.
(c) We have $\frac{x+y-1}{p} \in R$ for all $R \in V_s$ with $S \subset R$ and consequently

$$\left[\bigoplus_{i+k\leq m-3} \mathbf{Z}x^i\left(\frac{x+y-1}{p}\right)^k\right]\frac{\omega}{p} \subset \Omega^1_{R/\mathbf{Z}}.$$

This is also true for the $R \in V_s$ with $\tilde{S} \subset R$ since $x^i(\frac{x+y-1}{p})^k\frac{\omega}{p} = \tilde{x}^{m-3-i-k}(\frac{\tilde{x}-\tilde{y}-1}{p})^k\frac{\tilde{\omega}}{p}$. □

In the case $m \leq 5$ assertion (c) of the proposition holds with the equality sign as 4.5 and the examples in the next section show. In the general case $D_s^1(K_m)/D^1(K_m)$ is a nontrivial finite abelian group with the property that the order of each of its elements divides a power of m.

5. Examples

m = 4:

We claim that

$$D^1\left(\frac{K_4}{\mathfrak{d}}\right) = D_s^1(K_4) = \left(\mathbf{Z} \oplus \mathbf{Z}x \oplus \mathbf{Z}\frac{x+y-1}{2}\right)\frac{\omega}{2}.$$

Then by formula (1.1) of the introduction

$$D_s^1(K_4)/D^1(K_4) = (\mathbf{Z}_2)^2 \oplus \mathbf{Z}_4.$$

By 4.7(c) the group on the right side of the first equation is contained in $D_s^1(K_4)$.

Consider $R' := \mathbf{Z}[\frac{x}{2}]_{(2)}$. By 3.9 this ring is dominated by the localizations $R \in V_s(2)$ of $R'[w]$ with $w := \frac{y-1}{2}$ at its maximal ideals $(2, w)$ and $(2, w+1)$ and $\Omega^1_{R/\mathbf{Z}} = R\frac{\omega}{2}$. In the case $R = R'[w]_{(2,w)}$ we have $\frac{y-1}{4} = \frac{w}{2} \in R$ and the residues α of $\frac{x}{2}$ respectively β of $\frac{w}{2}$ satisfy $\alpha^4 + \beta = 0$ where α is transcendental over $\mathbf{F}_2$.

We apply Lemma 4.3. Let $M := \{1, 2, 2^2, \ldots\}$. Consider a differential $\eta := (a + bx + cy)\frac{\omega}{2}$ with $a, b, c \in \mathbf{Z}_M$. In order that $\eta \in D_s^1(K_4)$ the element $a+bx+cy = a+c+2b\frac{x}{2}+4c\frac{y-1}{4}$ must be in R, that is $v_2(a+c) \geq 0$, $v_2(b) \geq -1$. By exchanging the roles of x and y we obtain $v_2(a+b) \geq 0$ and $v_2(c) \geq -1$. The four conditions are only satisfied by the elements of $\mathbf{Z} \oplus \mathbf{Z}x \oplus \mathbf{Z}\frac{x+y-1}{2}$. This shows that $D_s^1(K_4) = (\mathbf{Z} \oplus \mathbf{Z}x \oplus \mathbf{Z}\frac{x+y-1}{2})\frac{\omega}{2}$.

The calculation of $D^1(\frac{K_4}{\mathfrak{d}})$ is more complicated. It is based on Remark 4.2. By 4.1 the differentials $\frac{\omega}{2}$ and $x\frac{\omega}{2} = -\frac{\tilde{\omega}}{2}$ are contained in $D^1(\frac{K_4}{\mathfrak{d}})$. In order to prove that $D^1(\frac{K_4}{\mathfrak{d}}) = D_s^1(K_4)$ we have to show that $\frac{x+y-1}{2}\frac{\omega}{2} \in D^1(\frac{K_4}{\mathfrak{d}})$. Consider a desingularization $Y \to X$ of the Fermat scheme X. Then according to 4.2 we have $D^1(\frac{K_4}{\mathfrak{d}}) = \cap\omega^1_{R/\mathbf{Z}}$ where the intersection is to be extended over all 1-dimensional local rings R of Y. For $R \in V_s$ it has been proved above that $\frac{x+y-1}{2}\frac{\omega}{2} \in D^1(K_4) \subset \omega^1_{R/\mathbf{Z}}$. If R is already a local ring of X, we can apply [5], formula (2) of Section 3. It states in the present case that $(\mathbf{Z} \oplus \mathbf{Z}x \oplus \mathbf{Z}y)\frac{\omega}{4} = H^0(X, \omega^1_{X/\mathbf{Z}})$. Therefore $(x + y - 1)\frac{\omega}{4} \in \omega^1_{R/\mathbf{Z}}$. It remains to be shown that $(x + y - 1)\frac{\omega}{4} \in \omega^1_{R/\mathbf{Z}}$ for the 1-dimensional local rings R of Y which are lying over a singularity of X and are not smooth over $\mathbf{Z}$. The only singularities of X in the case $m = 4$ are the maximal ideals $\mathfrak{m} := (2, x, y-1)$ and $\mathfrak{m}' := (2, x-1, y)$ of $S = \mathbf{Z}[x, y]/(x^4 + y^4 - 1)$. Resolving the singularities we shall show that only the following two rings R_1 and R_2 have to be studied, and the rings R_3 and R_4 arising from them by exchanging x and y.

(I) Construction of R_1 (see [5], Proof of 3.2 for a more general construction).

By $R' := (\mathbf{Z}[x]_{(2,x)}[Z]/(x^2Z - 2))_{(x)}$ a discrete valuation ring with quotient field $\mathbf{Q}(x)$ and residue field $\mathfrak{k}(R') = (\mathbf{F}_2[Z]/2\mathbf{F}_2[Z])_{(0)} \cong \mathbf{F}_2(Z)$ is given where Z is transcendental over $\mathbf{F}_2$.

Let $u := \frac{y-1}{x}$, $t := \frac{2}{x}$, $z := \frac{2}{x^2}$ and $R_1 := R'[u]$. Dividing the Fermat equation

$$(y-1)^4 + 4(y-1)^3 + 6(y-1)^2 + 4(y-1) + x^4 = 0 \tag{5.1}$$

by x^4 and using $2 = zx^2$ we obtain

$$u^4 + 2zxu^3 + 3zu^2 + z^2xu + 1 = 0 \tag{5.2}$$

an irreducible equation of integral dependence for u over R'. As

$$R_1/xR_1 = \mathbf{F}_2(Z)[U]/(U^4 + ZU^2 + 1) \cong \mathbf{F}_2(U)$$

is a field, R_1 is a discrete valuation ring with quotient field K_4, maximal ideal $\mathfrak{m}_{R_1} = (x)$ and residue field $\mathfrak{k}(R_1) = \mathbf{F}_2(U)$. In particular u and z are units of R_1 and $v_{R_1}(2) = 2$.

From $x^2z = 2$ and (5.2) we obtain for $\Omega^1_{R_1/\mathbf{Z}}$ the defining relations

$$tx^2z\mathrm{d}x + x^2\mathrm{d}z = 0$$

and

$$(2zu^3 + z^2u)\mathrm{d}x + (2xu^3 + 3u^2 + 2zxu)\mathrm{d}z + (4u^3 + 6zxu^2 + 6zu + z^2x)\mathrm{d}u = 0.$$

Therefore $\mathrm{d}z = -tz\mathrm{d}x$ in $[R_1, \mathrm{d}R_1]^1$. Further $2zu^3 + z^2u$ is a unit of R_1 and

$$4u^3 + 6zxu^2 + 6zu + z^2x = x(2tu^3 + 3txzu^2 + 3tzu + z^2)$$

where the expression in parentheses is also a unit. We obtain $[R_1, \mathrm{d}R_1]^1 = R_1\frac{\mathrm{d}x}{x} = R_1\frac{\omega}{x}$. Looking at the minors of the relation matrix we find that $\mathfrak{d}_1(R_1/\mathbf{Z}) = x^2R_1 = 2R_1$, hence $\omega^1_{R/\mathbf{Z}} = R_1\frac{\omega}{2x}$. Since $v_{R_1}(x) = 1$, $v_{R_1}(y-1) \geq 1$ and $v_{R_1}(2) = 2$ we have indeed $\frac{x+y-1}{2}\frac{\omega}{2} \in \omega^1_{R_1/\mathbf{Z}}$. By symmetry also $\frac{x+y-1}{2}\frac{\omega}{2} \in \omega^1_{R_3/\mathbf{Z}}$.

(II) Construction of R_2

Set $v := \frac{x}{t^3}$ and $R'' := \mathbf{Z}[x,t]_{(x,t)}[v]$. Since $\mathbf{Z}[x,t]_{(x,t)}$ is a two-dimensional regular local ring with maximal ideal (x,t) we have $R'' = \mathbf{Z}[x,t]_{(x,t)}[V]/(t^3V - x)$ and $R''/tR'' = \mathbf{F}_2[V]$. Therefore $R' := R''_{(t)}$ is a discrete valuation ring with quotient field $\mathbf{Q}(x)$ and residue field $\mathbf{F}_2(V)$ where V is transcendental over $\mathbf{F}_2$.

Dividing (5.1) by 2^3 and using $v = \frac{x}{t^3} = \frac{x^4}{2^3}$, $w = \frac{y-1}{2}$ we obtain

$$2w^4 + 4w^3 + 3w^2 + w + v = 0 \tag{5.3}$$

hence $R'[w] = R'[W]/(2W^4 + 4W^3 + 3W^2 + W + v)$ and

$$R'[w]/tR'[w] = \mathbf{F}_2(V)[W]/(W^2 + W + V) = \mathbf{F}_2(W)$$

where W is transcendental over $\mathbf{F}_2$. It follows that $R_2 := R'[w]$ is a discrete valuation ring with quotient field K_4, maximal ideal $\mathfrak{m}_{R_2} = (t)$ and residue field $\mathfrak{k}(R_2) = \mathbf{F}_2(W)$. We have the relations

$$v_{R_2}(t) = v_{R_2}(u) = v_{R_2}(tw) = 1, \qquad v_{R_2}(x) = v_{R_2}(vt^3) = 3, \qquad v_{R_2}(2) = 4. \tag{5.4}$$

By construction, the ring R_2 is a localization of

$$\mathbf{Z}[X, T, V, W]/(TX - 2, T^3V - X, 2W^4 + 4W^3 + 3W^2 + W + V).$$

Hence $\Omega^1_{R_2/\mathbf{Z}}$ has the defining relations

$$t\mathrm{d}x + x\mathrm{d}t = 0, \qquad -\mathrm{d}x + 3vt^2\mathrm{d}t + t^3\mathrm{d}v = 0, \qquad \mathrm{d}v + (1 + 6w + 12w^2 + 8w^3)\mathrm{d}w = 0.$$

In $[R_2, \mathrm{d}R_2]^1$ we then have the relations $\mathrm{d}x = -\frac{x}{t}\mathrm{d}t$, $\mathrm{d}v = -\frac{4x}{t^4}\mathrm{d}t$ and $\mathrm{d}w = -\epsilon^{-1}\mathrm{d}v$ where $\epsilon := 1+6w+12w^2+8w^3$ is a unit of R_2. It follows that $[R_2, \mathrm{d}R_2]^1 = R_2\mathrm{d}t$, and one also finds that $\mathfrak{d}_1(R_2/\mathbf{Z}) = t^4R_2$. We get

$$\omega^1_{R_2/\mathbf{Z}} = R_2\frac{\mathrm{d}t}{t^4} = R_2\frac{\mathrm{d}x}{xt^3} = R_2\frac{\omega}{2t^2}.$$

In particular $\frac{x+y-1}{2}\frac{\omega}{2} = (\frac{x}{2} + w)\frac{\omega}{2} \in \omega^1_{R_2/\mathbf{Z}}$, and by symmetry this is also true if R_2 is replaced by R_4.

(III) Desingularization of X

We shall show that the singularity $(2, x, y-1)$ of X can be resolved by a succession of two quadratic transformations (similarly for $(2, x-1, y)$) and that the R_i $(i = 1, \ldots, 4)$ are the only one-dimensional local rings on the desingularization lying over the singularities and not being smooth over $\mathbf{Z}$.

(a) Let $A_0 := S[\frac{x}{2}, \frac{y-1}{2}] = \mathbf{Z}[\frac{x}{2}, \frac{y-1}{2}]$. Dividing (5.1) by 2^3 we obtain with $x' := \frac{x}{2}$, $w = \frac{y-1}{2}$ the equation

$$2w^4 + 4w^3 + 3w^2 + w + 2(x')^4 = 0.$$

Then

$$A_0 = \mathbf{Z}[X', W]/(2W^4 + 4W^3 + 3W^2 + W + 2(X')^4)$$

and $A_0/2A_0 = \mathbf{F}_2[X', W]/(W(W+1))$. Therefore $\mathfrak{p}_1 := (2, w)$ and $\mathfrak{p}_2 := (2, w+1)$ are the prime ideals of height 1 in A_0 which contain $2A_0$. Since $(A_0)_{\mathfrak{p}_i}/2(A_0)_{\mathfrak{p}_i} \cong \mathbf{F}_2(W)$ are fields the $(A_0)_{\mathfrak{p}_i}$ $(i = 1, 2)$ are discrete valuation rings which are smooth over $\mathbf{Z}$. At maximal ideals which contain 2 the ring A_0 is regular.

(b) Let $A_1 := S[\frac{2}{x}, \frac{y-1}{x}] = \mathbf{Z}[x, t, u]$ where as earlier $t = \frac{2}{x}$, $u = \frac{y-1}{x}$. Dividing (5.1) by x^3 we obtain

$$xu^4 + 4u^3 + 3tu^2 + t^2u + x = 0. \tag{5.5}$$

The ring $\mathbf{Z}[x,t]=\mathbf{Z}[X,T]/(XT-2)$ is factorial ([8], Lemma 19.B) and $K_4=\mathbf{Q}(x)[U]/(h)$ where

$$h:=xU^4+4U^3+3tU^2+t^2U+x\in\mathbf{Z}[x,t][U].$$

Therefore h generates the kernel of $\mathbf{Z}[x,t][U]\to A_1$ $(U\mapsto u)$. Hence

$$A_1=\mathbf{Z}[X,T,U]/(XT-2,XU^4+4U^3+3TU^2+T^2U+X)$$

and

$$A_1/xA_1=\mathbf{F}_2[T,U]/(TU^2+T^2U)=\mathbf{F}_2[T,U]/(TU(T+U)).$$

The prime ideals of height 1 containing xA_1 are

$$\mathfrak{p}_1:=(x,t),\qquad \mathfrak{p}_2:=(x,u),\qquad \mathfrak{p}_3:=(x,t+u).$$

Further, xA_1 is contained in the maximal ideal $\mathfrak{M}:=(x,t,u)$ which is the only singularity of Spec A_1 lying over $(2,x,y-1)\subset S$.

The $(A_1)_{\mathfrak{p}_i}$ $(i=1,2,3)$ are discrete valuation rings whose maximal ideals are generated by x. Since t is a unit in $(A_1)_{\mathfrak{p}_i}$ for $i=2,3$ these rings are smooth over $\mathbf{Z}$. We show that $R:=(A_1)_{\mathfrak{p}_1}$ is the ring R_1 constructed in (I). Clearly $\mathbf{Z}[x]_{(2,x)}\subset R$ and $\mathfrak{k}(R)=\mathbf{F}_2(U)$. Therefore u^4+1 is a unit of R, and (5.5) shows that $v_R(t)=v_R(x)=1$, hence $v_R(2)=2$. It follows that $\mathbf{Z}[x]_{(2,x)}[\frac{2}{x^2}]\subset R$. By Eq. (5.2) we see that the residue of $z=\frac{2}{x^2}$ in $\mathfrak{k}(R)$ is $\frac{U^4+1}{U^2}$ which is transcendental over $\mathbf{F}_2$. It follows that $R\cap\mathbf{Q}(x)=\mathbf{Z}[x]_{(2,x)}[z]_{(x)}$. Further $u\in R$ and consequently $R_1=R$.

(c) Let $A_2:=S[\frac{2}{y-1},\frac{x}{y-1}]=\mathbf{Z}[y-1,s,\tilde{u}]$ with $s:=\frac{2}{y-1}$, $\tilde{u}:=\frac{x}{y-1}$. Substituting $2=s(y-1)$ and $x=\tilde{u}(y-1)$ into (5.1) and dividing by $(y-1)^3$ we obtain

$$y-1+s^2(y-1)^2+3s+s^2+\tilde{u}^4(y-1)=0.$$

We have

$$A_2=\mathbf{Z}[Y',S,\tilde{U}]/(SY'-2,Y'\tilde{U}^4+Y'+S^2(Y')^2+3S+S^2)$$

and $A_2/(y-1)A_2=\mathbf{F}_2[S,\tilde{U}]/(S(S+1))$. The prime ideals of height 1 in A_2 containing $(y-1)A_2$ are

$$\mathfrak{q}_1:=(y-1,s),\qquad \mathfrak{q}_2:=(y-1,s+1)$$

and the $(A_2)_{\mathfrak{q}_i}$ $(i=1,2)$ are discrete valuation rings whose maximal ideals are generated by $y-1$. Since s is a unit and $2=s(y-1)\in(A_2)_{\mathfrak{q}_2}$ this ring is smooth over $\mathbf{Z}$. In $(A_2)_{\mathfrak{q}_1}$ the element $\tilde{u}$ is a unit, and it follows that $(A_2)_{\mathfrak{q}_1}=(A_1)_{\mathfrak{p}_1}=R_1$, the ring constructed in (I). There are no singularities in Spec A_2 containing $(y-1)A_2$.

(d) Now we blow up $A_1=\mathbf{Z}[x,t,u]$ at the maximal ideal $\mathfrak{M}=(x,t,u)$ in order to resolve this singularity.

Set $A_{10}:=A_1[\frac{x}{u},\frac{t}{u}]$ and $\bar{x}:=\frac{x}{u}$, $\bar{t}:=\frac{t}{u}$. Then $A_{10}=\mathbf{Z}[u,\bar{x},\bar{t}]$. Dividing (5.5) by u and using $t=\bar{t}u$, $x=\bar{x}u$ we obtain

$$\bar{x}u^4+4u^2+3\bar{t}u^2+\bar{t}^2u^2+\bar{x}=0$$

in particular $\bar{x}\in uA_{10}$. We show that uA_{10} is a prime ideal of A_{10} and $(A_{10})_{(u)}=R_2$, the ring constructed in (II).

By (5.4) we have that $A_{10}\subset R_2$ and $u\in\mathfrak{m}_{R_2}\cap A_{10}=:\mathfrak{p}$. Further $A_{10}/uA_{10}=\mathbf{F}_2[\tau]$ with the residue τ of $\bar{t}$. Let W be the residue of $w=\frac{u}{t}=\bar{t}^{-1}$. By the composed map

$$A_{10}/uA_{10}\to A_{10}/\mathfrak{p}\to R_2/\mathfrak{m}_{R_2}=\mathbf{F}_2(W)$$

the element τ is mapped onto W^{-1}. Hence τ is transcendental over $\mathbf{F}_2$ and uA_{10} a prime ideal. It follows that $(A_{10})_{(u)}$ is a discrete valuation ring, necessarily $(A_{10})_{(u)}=R_2$. Since $A_{10}/uA_{10}=\mathbf{F}_2[\tau]$ is a polynomial ring there are no singularities in Spec A_{10} which contain uA_{10}.

Consider now $A_{11}:=A_1[\frac{t}{x},\frac{u}{x}]=\mathbf{Z}[x,\frac{2}{x^2},\frac{y-1}{x^2}]$. From (5.1) we obtain

$$x^4\left(\frac{y-1}{x^2}\right)^4+4x^2\left(\frac{y-1}{x^2}\right)^3+3x^2\left(\frac{2}{x^2}\right)\left(\frac{y-1}{x^2}\right)^2+x^2\left(\frac{2}{x^2}\right)^2\left(\frac{y-1}{x^2}\right)+1=0.$$

Therefore x is a unit of A_{11} and the fiber over xA_{11} is empty.

Finally let $A_{12} := A_1[\frac{x}{t}, \frac{u}{t}] = \mathbf{Z}[t, \frac{x}{t}, w]$. This is a subring of R_2. Also here one shows that tA_{12} is a prime ideal of A_{12} and $R_2 = (A_{12})_{(t)}$. In fact, dividing (5.5) by t^3 we see that $v = \frac{x}{t^3}$ satisfies $v = -(2w^4 + 4w^3 + 3w^2 + w)$. Therefore $\frac{x}{t} = t^2 v \in tA_{12}$ and $A_{12}/tA_{12} = \mathbf{F}_2[\Omega]$ with the residue Ω of w. By the composed map

$$A_{12}/tA_{12} \to A_{12}/\mathfrak{m}_{R_2} \cap A_{12} \to R_2/\mathfrak{m}_{R_2} = \mathbf{F}_2(W)$$

Ω is mapped onto W, hence Ω is transcendental over $\mathbf{F}_2$. We see that $(A_{12})_{(t)} = R_2$ and that there are no singularities in Spec A_{12} which contain tA_{12}.

We have resolved the singularity $\mathfrak{m} = (2, x, y-1)$ of X, and we have seen that R_1 and R_2 are the only discrete valuation rings at points of the fiber over $\mathfrak{m}$ which are not smooth over $\mathbf{Z}$. Arguing similarly for $\mathfrak{m}' = (2, x-1, y)$ we find the analogous rings R_3 and R_4. Thanks to Remark 4.2 and what was said in (I) and (II) the desired formula for $D^1(\frac{K_4}{\mathfrak{d}})$ follows.

$\mathbf{m} = 5$:

We claim that

$$D_s^1(K_5) = \left[\mathbf{Z} \oplus \mathbf{Z}x \oplus \mathbf{Z}x^2 \oplus \mathbf{Z}\frac{x+y-1}{5} \oplus \mathbf{Z}x\frac{x+y-1}{5} \oplus \mathbf{Z}\left(\frac{x+y-1}{5}\right)^2\right]\frac{\omega}{5}.$$

From formulas (1.1) respectively (1.2) of the introduction it follows then that

$$D_s^1(K_5)/D^1(K_5) = (\mathbf{Z}_5)^3 \oplus (\mathbf{Z}_{25})^2 \oplus \mathbf{Z}_{125} \quad \text{and} \quad D_s^1(K_5)/D^1\left(\frac{K_5}{\mathfrak{d}}\right) = (\mathbf{Z}_5)^2 \oplus \mathbf{Z}_{25}.$$

By 4.7(c) the group on the right side of the first equation is contained in $D^1(K_5)$.

Consider $R' := \mathbf{Z}[\frac{x}{5}]_{(5)}$ and $R := R'[\frac{x+y-1}{5}] \in V_s(5)$. Then we have $v := \frac{y-1}{5^4} \in R$ by 3.6(b), and with $u := \frac{x}{5}$ the residues $\bar{u}, \bar{v}$ of u, v in $\mathfrak{k}(R)$ satisfy $\bar{u}^5 + \bar{v} = 0$ where $\bar{u}$ is transcendental over $\mathbf{F}_2$. Moreover $\Omega^1_{R/\mathbf{Z}} = R\frac{\omega}{5}$.

We apply Lemma 4.3. Let $M := \{1, 5, 5^2, \ldots\}$. Consider the differential $\eta := l\frac{\omega}{5}$ with $l := \sum_{i+k\le 2} a_{ik}x^i y^k$ where $a_{ik} \in \mathbf{Z}_M$. In order that $\eta \in D_s^1(K_5)$ we must have $l \in R$. Write

$$\begin{aligned} l &= a_{00} + a_{01} + a_{02} + 5(a_{10} + a_{11})\frac{x}{5} + 5^2 a_{20}\left(\frac{x}{5}\right)^2 \\ &\quad + 5^4(a_{01} + 2a_{02})\frac{y-1}{5^4} + 5^5 a_{11}\frac{x}{5}\frac{y-1}{5^4} + 5^8 a_{02}\left(\frac{y-1}{5^4}\right)^2. \end{aligned}$$

If $l \in R$, then in particular

$$v_5(a_{00} + a_{01} + a_{02}) \ge 0, \qquad v_5(a_{10} + a_{11}) \ge -1, \qquad v_5(a_{20}) \ge -2. \tag{5.6}$$

Exchanging the roles of x and y we obtain the conditions

$$v_5(a_{00} + a_{10} + a_{20}) \ge 0, \qquad v_5(a_{01} + a_{11}) \ge -1, \qquad v_5(a_{02}) \ge -2. \tag{5.7}$$

Now let $R' := \mathbf{Z}[\frac{\tilde{x}}{5}]_{(5)}$, $R := R'[\frac{\tilde{y}-\tilde{x}+1}{5}]$. Since $l\frac{\omega}{5} = -\tilde{l}\frac{\tilde{\omega}}{5}$ with

$$\begin{aligned} \tilde{l} := \tilde{x}^2 l &= a_{20} + a_{10}\tilde{x} + a_{00}\tilde{x}^2 + a_{11}\tilde{y} + a_{01}\tilde{x}\tilde{y} + a_{02}\tilde{y}^2 \\ &= a_{20} - a_{11} + a_{02} + 5(a_{10} - a_{01})\frac{\tilde{x}}{5} + 5^2 a_{00}\left(\frac{\tilde{x}}{5}\right)^2 \\ &\quad + 5^4(a_{11} - 2a_{02})\frac{\tilde{y}+1}{5^4} + 5^5 a_{01}\frac{\tilde{x}}{5}\frac{\tilde{y}+1}{5^4} + 5^8 a_{02}\left(\frac{\tilde{y}+1}{5^4}\right)^2 \end{aligned}$$

we get from $l\frac{\omega}{5} \in \Omega^1_{R/\mathbf{Z}} = R\frac{\omega}{5}$ the conditions

$$v_5(a_{20} + a_{02} - a_{11}) \ge 0, \qquad v_5(a_{10} - a_{01}) \ge -1, \qquad v_5(a_{00}) \ge -2. \tag{5.8}$$

With these it follows from (5.6) and (5.7) at first that $v_5(a_{20}-a_{02}) \geq -1$, then $v_5(a_{11}) \geq -2$ and finally $v_5(a_{ik}) \geq -2$ for all (i,k).

Now consider $R' := \mathbf{Z}[x]_{(5,x^2-x+1)}[\frac{x^2-x+1}{5}]_{(5)}$ and $R := R'[w]$ with $w := \frac{x+y-1}{5}$. Set $u := \frac{x^2-x+1}{5}$ and denote the residues of u, w, x in $\mathfrak{k}(R)$ by $\bar{u}, \bar{w}, \xi$. We have $\mathfrak{k}(R') = \mathbf{F}_5[\xi](\bar{u})$ where $\bar{u}$ is transcendental over $\mathbf{F}_5[\xi]$. Further $(1-\xi)^4\bar{w} = \bar{u}$, hence $\bar{w}$ is also transcendental over $\mathbf{F}_5[\xi]$. Write

$$\begin{aligned} l &= a_{02}(x+y-1)^2 + (a_{11}-2a_{02})x(x+y-1) + (a_{01}+2a_{02})(x+y-1) \\ &\quad + (a_{20}-a_{11}+a_{02})(x^2-x+1) + (a_{10}-a_{01}+a_{20}-a_{02})x + (a_{00}+a_{11}+a_{01}-a_{20}) \\ &= 5^2a_{02}w^2 + 5(a_{11}-2a_{02})xw + 5(a_{01}+2a_{02})w + 5(a_{20}-a_{11}+a_{02})u \\ &\quad + (a_{10}-a_{01}+a_{20}-a_{02})x + (a_{00}+a_{11}+a_{01}-a_{20}). \end{aligned}$$

According to (5.6)–(5.8) the terms 5^2a_{02}, $5(a_{20}+a_{02}-a_{11})u$, $(a_{10}-a_{01}+a_{20}-a_{02})x$ belong to R. In order that $l \in R$ the following conditions must be satisfied

$$v_5(a_{11}-2a_{02}) \geq -1, \qquad v_5(a_{01}+2a_{02}) \geq -1, \qquad v_5(a_{00}+a_{11}+a_{01}-a_{20}) \geq 0. \tag{5.9}$$

Formulas (5.7) and the last relation imply

$$v_5(a_{00}-a_{20}) \geq -1. \tag{5.10}$$

The conditions show that if $v_5(a_{ik}) \geq -1$ for one pair (i,k), then this holds for all (i,k). If we set $a_{00} = a_{20} = a_{02} = \frac{1}{5^2}$, $a_{10} = a_{01} = -\frac{2}{5^2}$, $a_{11} = \frac{2}{5^2}$, then the conditions (5.6)–(5.10) are satisfied. To this choice of the a_{ik} corresponds the differential

$$\left(\frac{x+y-1}{5}\right)^2 \frac{\omega}{5} \in D_s^1(K_5).$$

Write $[l - 5^2a_{02}(\frac{x+y-1}{5})^2]\frac{\omega}{5} = [\sum_{i+k\leq 2} b_{ik}x^iy^k]\frac{\omega}{5}$ with $b_{ik} \in \mathbf{Z}_M$, $b_{02} = 0$. Then we have $v_5(b_{ik}) \geq -1$ for all (i,k) and moreover by the conditions analogous to (5.6)–(5.8) the conditions

$$v_5(b_{00}+b_{01}) \geq 0, \qquad v_5(b_{00}+b_{10}+b_{20}) \geq 0, \qquad v_5(b_{20}-b_{11}) \geq 0$$

are satisfied. Subtracting $5b_{11}\frac{x+y-1}{5}\frac{\omega}{5}$ we are left with the conditions

$$v_5(b_{00}+b_{01}) \geq 0, \qquad v_5(b_{00}+b_{10}) \geq 0, \qquad v_5(b_{20}) \geq 0$$

and subtracting $5b_{01}\frac{x+y-1}{5}\frac{\omega}{5}$ it follows that $b_{00}, b_{10}, b_{20} \in \mathbf{Z}$. This shows that each element of $D_s^1(K_5)$ has the form stated at the beginning.

m = 6:

We claim that

$$\begin{aligned} D_s^1(K_6) = \Bigg[&\mathbf{Z}\frac{xy}{6} \oplus \mathbf{Z}\frac{x^2y}{2} \oplus \mathbf{Z}\frac{xy^2}{2} \oplus \mathbf{Z}\frac{x^3+y^3-1}{2} \\ &\oplus \mathbf{Z}x\frac{x^2+y^2-1}{3^2} \oplus \mathbf{Z}y\frac{x^2+y^2-1}{3^2} \oplus \mathbf{Z}\frac{x^2+y^2-1}{3^2} \oplus \mathbf{Z}x^2 \oplus \mathbf{Z}x \oplus \mathbf{Z}\Bigg]\frac{\omega}{6}. \end{aligned}$$

Then it follows from formulas (1.1) and (1.2) of the introduction that

$$D_s^1(K_6)/D^1(K_6) = (\mathbf{Z}_2)^6 \oplus (\mathbf{Z}_4)^4 \oplus (\mathbf{Z}_3)^6 \oplus \mathbf{Z}_9 \oplus (\mathbf{Z}_{27})^3$$

and

$$D_s^1(K_6)/D^1\left(\frac{K_6}{\mathfrak{d}}\right) = (\mathbf{Z}_2)^4 \oplus \mathbf{Z}_3 \oplus (\mathbf{Z}_9)^3.$$

Denote the group on the right side of the first equation by $(*)$. By formulas (1.2) and (1.3) of the introduction and by 4.7(b) we know already that

$$x^i\frac{\omega}{6}\ (i=0,1,2), \qquad \frac{x^3+y^3-1}{2}\frac{\omega}{6} \quad \text{and} \quad \frac{x^2+y^2-1}{3^2}\frac{\omega}{6}$$

are elements of $D_s^1(K_6)$. Let $R \in V_s(p)$ with $p \in \{2, 3\}$. If $S \subset R$, then $xy \in \mathfrak{m}_R$ by 3.3(a) and (b), and it follows that $(*) \subset \omega^1_{R/\mathbf{Z}}$ for these R.

Consider now $R \in V_s(p)$ with $v_R(\tilde{x}) > 0$. Then $p = 3$ by 3.11, and we have $\frac{\tilde{x}\tilde{y}}{6} \in R$ and $\frac{\tilde{x}^2-\tilde{y}^2-1}{3^2} \in R$ by 3.10. Further $\frac{\tilde{\omega}}{6} \in \omega^1_{R/\mathbf{Z}}$ by 4.7(a). Now $\omega = -\tilde{x}^3\tilde{\omega}$ implies that

$$\frac{xy}{6}\frac{\omega}{6} = -\frac{\tilde{x}\tilde{y}}{6}\frac{\tilde{\omega}}{6}, \qquad \frac{x^2y}{2}\frac{\omega}{6} = -\frac{\tilde{y}}{2}\frac{\tilde{\omega}}{6}, \qquad \frac{xy^2}{2}\frac{\omega}{6} = -\frac{\tilde{y}^2}{2}\frac{\tilde{\omega}}{6}$$

and

$$x\frac{x^2+y^2-1}{3^2}\frac{\omega}{6} = \frac{\tilde{x}^2-\tilde{y}^2-1}{3^2}\frac{\tilde{\omega}}{6}, \qquad y\frac{x^2+y^2-1}{3^2}\frac{\omega}{6} = \tilde{y}\frac{\tilde{x}^2-\tilde{y}^2-1}{3^2}\frac{\tilde{\omega}}{6}$$

are in $\omega^1_{R/\mathbf{Z}}$. Therefore $(*) \subset D_s^1(K_6)$. With similar arguments as in the case $m = 5$, but with longer calculations, one can show that also the opposite inclusion holds.

References

[1] S. Abhyankar, On the valuations centered in a local domain, Amer. J. Math. 78 (1956) 321–348.
[2] R. Berndt, Arithmetisch ganze Differentiale, Abh. Math. Sem. Univ. Hamburg 47 (1978) 249–270.
[3] J.-B. Bost, A neglected aspect of Kähler's work in arithmetic geometry: Birational invariants of algebraic varieties over number fields, in: R. Berndt, O. Riemenschneider (Eds.), Erich Kähler. Mathematische Werke. Mathematical Works, De Gruyter, Berlin, 2003, pp. 854–869.
[4] E. Kähler, Geometria aritmetica, Annali di Mat. 45 (1958).
[5] E. Kunz, R. Waldi, On Kähler's integral differential forms of arithmetic function fields, Abh. Math. Sem. Univ. Hamburg 73 (2003) 297–310.
[6] E. Kunz, R. Waldi, Integral differentials of elliptic function fields, Abh. Math. Sem. Univ. Hamburg 74 (2004) 243–252.
[7] H. Maeda, Wild singularities of the Fermat curve over **Z**, in: Algebra, Arithmetic and Geometry with Applications (Papers from Shreeram S. Abhyankars 70th Birthday Conference), Springer, 2004, pp. 609–618.
[8] H. Matsumura, Commutative Algebra, second ed., Benjamin/Cummings, 1980.
[9] M. Nagata, A theorem on valuation rings and its applications, Nagoya Math. J. 29 (1967) 85–91.
[10] P. Ribenboim, Fermat's Last Theorem for Amateurs, Springer, New York, 1999.